Introduction

Computers and the Internet have entered the mainstream of American life. Millions of Americans spend hours every day using computers and mobile devices to send and receive email, surf the Internet, maintain databases, and participate in countless other activities.

Unfortunately, those who commit crimes have not missed the information revolution. Criminals use mobile phones, laptop computers, and network servers in the course of committing their crimes. In some cases, computers provide the means of committing crime. For example, the Internet can be used to deliver a death threat via email; to launch hacker attacks against a vulnerable computer network, to disseminate computer viruses, or to transmit images of child pornography. In other cases, computers merely serve as convenient storage devices for evidence of crime. For example, a drug dealer might keep a list of who owes him money in a file stored in his desktop computer at home, or a money laundering operation might retain false financial records in a file on a network server. Indeed, virtually every class of crime can involve some form of digital evidence.

The dramatic increase in computer-related crime requires prosecutors and law enforcement agents to understand how to obtain electronic evidence stored in computers. Electronic records such as computer network logs, email, word processing files, and image files increasingly provide the government with important (and sometimes essential) evidence in criminal cases. The purpose of this publication is to provide Federal law enforcement agents and prosecutors with systematic guidance that can help them understand the legal issues that arise when they seek electronic evidence in criminal investigations.

The law governing electronic evidence in criminal investigations has two primary sources: the Fourth Amendment to the U.S. Constitution, and the statutory privacy laws codified at 18 U.S.C. §§ 2510-22, 18 U.S.C. §§ 2701-12, and 18 U.S.C. §§ 3121-27. Although constitutional and statutory issues overlap in some cases, most situations present either a constitutional issue under the Fourth Amendment or a statutory issue under these three statutes. This manual reflects that division: Chapters 1 and 2 address the Fourth Amendment law of search and seizure, and Chapters 3 and 4 focus on the statutory issues, which arise mostly in cases involving computer networks and the Internet.

Chapter 1 explains the restrictions that the Fourth Amendment places on the warrantless search and seizure of computers and computer data. The chapter begins by explaining how the courts apply the "reasonable expectation of privacy" test to computers, turns next to how the exceptions to the warrant requirement apply in cases involving computers, and concludes with a comprehensive discussion of the difficult Fourth Amendment issues raised by warrantless workplace searches of computers. Questions addressed in this chapter include: When does the government need a search warrant to search and seize a suspect's computer? Can an investigator search without a warrant through a suspect's mobile phone seized incident to arrest? Does the government need a warrant to search a government employee's desktop computer located in the employee's office?

Chapter 2 discusses the law that governs the search and seizure of computers pursuant to search warrants. The chapter begins by briefly addressing the different roles computers can play in criminal offenses and the goals investigators and prosecutors should keep in mind when drafting search warrants. It then addresses issues that arise in drafting search warrants, in the forensic analysis of computers seized pursuant to warrants, and in post-seizure challenges to the search process. Finally, it addresses special limitations on the use of search warrants to search computers, such as the limitations imposed by the Privacy Protection Act, 42 U.S.C. § 2000aa. Questions addressed in the chapter include: How should prosecutors draft search warrant language so that it complies with the particularity requirement of the Fourth Amendment and Rule 41 of the Federal Rules of Criminal Procedure? What are the time requirements for the review of computers seized pursuant to a search warrant? What is the law governing when the government must search and return seized computers?

The focus of Chapter 3[1] is the Stored Communications Act, 18 U.S.C. §§ 2701-12 ("SCA"). The SCA governs how investigators can obtain stored account records and contents from network service providers, including Internet service providers ("ISPs"), telephone companies, and cell phone service providers. SCA issues arise often in cases involving the Internet: when investigators seek stored information concerning Internet accounts from providers of Internet service,

[1] In previous versions of this Manual, the SCA was referred to as the Electronic Communications Privacy Act. The SCA was included as Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), but ECPA itself also included amendments to the Wiretap Act and created the Pen Register and Trap and Trace Devices statute addressed in Chapter 4. *See* Pub. L. No. 99-508, 100 Stat. 1848 (1986). In this Manual, "the SCA" will refer to 18 U.S.C. §§ 2701-12, and "ECPA" will refer to the 1986 statute.

they must comply with the statute. Topics covered in this section include: How can the government obtain email and account logs from ISPs? When does the government need to obtain a search warrant, as opposed to an 18 U.S.C. § 2703(d) order or a subpoena? When can providers disclose email and records to the government voluntarily? What remedies will courts impose when the SCA has been violated?

Chapter 4 reviews the legal framework that governs electronic surveillance, with particular emphasis on how the statutes apply to surveillance on communications networks. In particular, the chapter discusses the Wiretap Act, 18 U.S.C. §§ 2510-22 (referred to here as "Title III"), as well as the Pen Register and Trap and Trace Devices statute, 18 U.S.C. §§ 3121-27. These statutes govern when and how the government can conduct real-time surveillance, such as monitoring a computer hacker's activity as he breaks into a government computer network. Topics addressed in this chapter include: When can victims of computer crime monitor unauthorized intrusions into their networks and disclose that information to law enforcement? Can network "banners" generate consent to monitoring? How can the government obtain a pen register/trap and trace order that permits the government to collect packet header information from Internet communications? What remedies will courts impose when the electronic surveillance statutes have been violated?

Of course, the issues discussed in Chapters 1 through 4 can overlap in actual cases. An investigation into computer hacking may begin with obtaining stored records from an ISP according to Chapter 3, move next to an electronic surveillance phase implicating Chapter 4, and then conclude with a search of the suspect's residence and a seizure of his computers according to Chapters 1 and 2. In other cases, agents and prosecutors must understand issues raised in multiple chapters not just in the same case, but at the same time. For example, an investigation into workplace misconduct by a government employee may implicate all of Chapters 1 through 4. Investigators may want to obtain the employee's email from the government network server (implicating the SCA, discussed in Chapter 3); may wish to monitor the employee's use of the telephone or Internet in real-time (raising surveillance issues from Chapter 4); and may need to search the employee's desktop computer in his office for clues of the misconduct (raising search and seizure issues from Chapters 1 and 2). Because the constitutional and statutory regimes can overlap in certain cases, agents and prosecutors will need to understand not only all of the legal issues covered in Chapters 1 through 4, but will also need to understand the precise nature of the information to be gathered in their particular cases.

Chapters 1 through 4 are followed by Chapter 5, which discusses evidentiary issues that arise frequently in computer-related cases. Prosecutors should always be concerned with admissibility issues that may arise in court proceedings. Chapter 5 addresses both hearsay and Confrontation Clause issues associated with computer records. It then discusses authentication of computer-stored records and records created by computer processes, including common challenges to authenticity, such as claims that computer records have been tampered with. It also discusses the best evidence rule and the use of summaries containing electronic evidence. Questions addressed in this chapter include: When are computer-generated records not hearsay? How can the contents of a website be authenticated? This Manual then concludes with appendices that offer sample forms, letters, and orders.

Computer crime investigations raise many novel issues. Agents and prosecutors who need more detailed advice can rely on several resources for further assistance. At the federal district level, every United States Attorney's Office has at least one Assistant United States Attorney who has been designated as a Computer Hacking and Intellectual Property ("CHIP") attorney. Every CHIP attorney receives extensive training in computer crime issues and is primarily responsible for providing expertise relating to the topics covered in this manual within his or her district. CHIPs may be reached in their district offices. Further, several sections within the Criminal Division of the United States Department of Justice in Washington, D.C., have expertise in computer-related fields. The Office of International Affairs ((202) 514-0000) provides expertise in the many computer crime investigations that raise international issues. The Office of Enforcement Operations ((202) 514-6809) provides expertise in the wiretapping laws and other privacy statutes discussed in Chapters 3 and 4. Also, the Child Exploitation and Obscenity Section ((202) 514-5780) provides expertise in computer-related cases involving child pornography and child exploitation.

Finally, agents and prosecutors are always welcome to contact the Computer Crime and Intellectual Property Section ("CCIPS") directly both for general advice and specific case-related assistance. During regular business hours, a CCIPS attorney is on duty to answer questions and provide assistance to agents and prosecutors on the topics covered in this document, as well as other matters that arise in computer crime cases. The main number for CCIPS is (202) 514-1026. After hours, CCIPS can be reached through the Justice Command Center at (202) 514-5000.